UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/038,169	01/02/2002	Dan Boneh	200634-0096-00-US (425599	7811

23973   7590   03/31/2009
DRINKER BIDDLE & REATH
ATTN: INTELLECTUAL PROPERTY GROUP
ONE LOGAN SQUARE
18TH AND CHERRY STREETS
PHILADELPHIA, PA 19103-6996

EXAMINER
TO, BAOTRAN N

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
03/31/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/038,169	BONEH ET AL.
Office Action Summary	Examiner	Art Unit	
	Baotran N. To	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>25 August 2008 and 08 December 2008</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>31-55</u> is/are pending in the application.

    4a) Of the above claim(s) <u>1-32 (Canceled)</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>31-55</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

08/25/2008 has been entered.

This Office action is in response to the Applicant's Amendment filed 08/25/2008.

Claims 1-31 are canceled.

Claims 32-55 are newly added.

Claims 32-55 are presented for examination.

Election/Restrictions

2.   Applicant's election with traverse of Invention II – Claim 52 in the reply filed on

12/08/2008 is acknowledged. The traversal is on the ground(s) that Claim 52

designated invention II overlaps in scope with at least designated invention I of Claim

32. Applicant's arguments, see Remarks, filed 12/08/2008, with respect to Claims 32-

55 have been fully considered and are persuasive. The Restriction of Claims 32-55 has

been withdrawn.

Response to Arguments

3.　　Applicant's arguments with respect to claims 32-55 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.　　Claims 32-33, 35-41, 44, 46-49, and 53-55 are rejected under 35 U.S.C. 102(e)

as being anticipated by Wessman (U.S. Patent 7,111,005 B1) hereinafter Wessman.

Regarding Claims 32, 44, 53, and 55, Wessman discloses a transparent

encryption appliance/system/method/medium for protecting data stored in a web server

environment that does not secure by encrypting, hashing, or keyed hashing data

received from the web before it is stored (Figures 1 and 2), comprising:

at least one network interface for coupling to at least one network and

communicating with one or more clients via the at least one network (Figures 1 and 2,

interface between elements 110 and 112);

a server interface for coupling to a web server environment, wherein the server interface and the at least one network interface communicate using the same communications protocol (Figures 1 and 2, interface betweens element 112 and 118); and

a processor coupled to the at least one network interface and the server interface for at least one of securing and unsecuring data (Figures 1 and 2, element 112), wherein:

securing data comprises: identifying first sensitive data contained in a data transaction received through the at least one network interface (col. 1, lines 15-17); securing the sensitive data by at least one of encrypting, hashing, and keyed hashing (Figure 6, element 602); replacing in the data transaction the identified sensitive data with the secured sensitive data (Figure 6, element 610, col. 1, lines 15-17 and col. 6, line 9); and providing the data transaction including the secured sensitive data to the web server environment, wherein the secured sensitive data is stored in the web server environment (Figure 6, elements 606 and 612, col. 6, lines 10-12); and

unsecuring data comprises: responsive to a request (a request from client 110) received through the at least one network interface for sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data (Figure 7, element 702, col. 6, lines 17-18), receiving from the web server environment the secured sensitive data corresponding to the requested data (Figure 7, element 704, col. 6, lines 18-19); unsecuring the received secured data by at least one of decrypting and hash verifying (Figure 7, element 712, col. 6, lines 31-32); and

providing the unsecured sensitive data through the at least one network interface

(Figure 7, element 714, col. 6, lines 32-33).

Regarding Claim 33, Wessman discloses the limitations of Claim 32 above.

Wessman further discloses wherein: in securing data the data transaction is received

through a first interface (Figures 6); and

in unsecuring data the request is received, and the unsecured data is provided

through, the first interface or a second interface (Figure 7).

Regarding Claims 35 and 46, Wessman discloses the limitations of Claim 32

above. Wessman further discloses wherein the received data transaction is one of a

cleartext transaction and a Hypertext Transfer Protocol (HTTP) transaction (Figure 6,

element 602).

Regarding Claim 36, Wessman discloses the limitations of Claim 32 above.

Wessman further discloses wherein the at least one network is at least one of the

Internet, a wired network type, a wireless network type, a hybrid network type, an

independent network, a proprietary network, or a back plane network (Figures 1 and 2).

Regarding Claims 37 and 47, Wessman discloses the limitations of Claim 32

above. Wessman further discloses a key storage for storing at least one cryptographic

key for use in at least one of the securing and unsecuring of data (Figure 1, elements

116 and 120, col. 3, lines 52-58).

Regarding Claims 38-39 and 48, Wessman discloses the limitations of Claim 32

above. Wessman further discloses above a user interface for use in loading the at least

one key into the key storage and wherein the user interface is further for use in

specifying access controls to the stored keys (Figure 1, elements 116 and 120, col. 3,

lines 52-58).

Regarding Claims 40-41 and 49, Wessman discloses the limitations of Claim 32

above. Wessman further discloses above a user interface for use in specifying one or

more fields containing the sensitive data wherein the one or more fields are identified by

one or more regular expressions (col. 5, lines 30-63).

Regarding Claim 54, Wessman discloses the limitations of Claim 53 above.

Wessman further discloses after the storing step: responsive to request for at least a

portion of the sensitive data, retrieving the stored secured sensitive data corresponding

to the request sensitive data (Figure 7, element 704, col. 6, lines 18-19); unsecuring the

retrieved sensitive data by at least one of decrypting and hash verifying (Figure 7,

element 712, col. 6, lines 31-32); and providing the unsecured sensitive data to fulfill the

request (Figure 7, element 714, col. 6, lines 32-33).

5.   Claims 43 and 51 are rejected under 35 U.S.C. 102(e) as being anticipated by

Rollins (U.S. Patent 7,415,429 B2) hereinafter Rollins.

        Regarding Claims 43 and 51, Rollins discloses a transparent encryption

appliance/system for protecting data provided by a web server environment that does

not secure data generated by the web server environment, comprising:

        at least one network interface for coupling to at least one network and

communicating with one or more clients via the at least one network (Figure 3, interface

between elements 303 and 308);

        a server interface for coupling to a web server environment, wherein the server

interface and the at least one network interface communicate using the same

communications protocol (SSL) (Figure 3, interface between elements 308 and 306 and

Figures 7A and 7B, interface between elements 708, 706 and 714); and

        a processor coupled to the at least one network interface and the server interface

for at least one of securing and unsecuring data (Figure 3, element 708), wherein:

        securing a cookie comprises: identifying a cookie received through the server

interface (col. 14, lines 66-67 and col. 18, lines 13-15); securing the cookie by at least

one of encrypting, hashing, and keyed hashing the cookie (col. 20, lines 1-25); and

providing the secured cookie to a client computer through the at least one network

interface, wherein the secured cookie is stored in the client computer (col. 20, lines 1-

25); and

unsecuring a cookie comprises: responsive to a request received through the

server interface for a cookie stored on a client computer (col. 18, lines 13-20), receiving

from the client computer the secured cookie corresponding to the requested cookie

through the at least one network interface (col. 20, lines 38-46); unsecuring the received

secured cookie by at least one of decrypting and hash verifying (col. 20, lines 16-21);

and providing the unsecured cookie through the server interface (col. 18, lines 61-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 34, 42, 45, and 50 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Wessman as Claims 32 and 44 and further in view of Rollins (U.S.

Patent 7,415,429 B2) hereinafter Rollins.

Regarding Claims 34 and 45, Wessman discloses the limitations of Claim 32

above. Wessman does not disclose wherein the processor manages SSL traffic and

handles computations that support SSL connections, wherein at least one of: in

securing data the data transaction is received via a first SSL connection and SSL

computations are completed before identifying the first sensitive data contained in the

data transaction; and in unsecuring data the unsecured data is provided via a second

SSL connection. However, Rollins expressly disclose the above features. Therefore,

One of ordinary skill in the art at the time the invention was made to have incorporated

Rollins within Wessman to include SSL connection in order to provide enhanced

security.

Regarding Claims 42 and 50, Wessman discloses the limitations of Claim 32

above. Wessman does not disclose wherein the appliance secures and unsecures web

cookies provided by the web server environment, wherein: securing a cookie comprises:

identifying a cookie received through the server interface; securing the cookie by at

least one of encrypting, hashing, and keyed hashing the cookie; and providing the

secured cookie to one of the one or more clients through the at least one network

interface, wherein the secured cookie is stored in the client; and unsecuring the cookie

comprises: responsive to a request received through the server interface for the cookie

stored on a client, receiving from the client the secured cookie corresponding to the

requested cookie through the at least one network interface; unsecuring the received

secured cookie by at least one of decrypting and hash verifying; and providing the

unsecured cookie through the server interface.

However, Rollins expressly discloses securing a cookie comprises: identifying a

cookie received through the server interface (col. 14, lines 66-67 and col. 18, lines 13-

15); securing the cookie by at least one of encrypting, hashing, and keyed hashing the

cookie (col. 20, lines 1-25); and providing the secured cookie to a client computer

through the at least one network interface, wherein the secured cookie is stored in the

client computer (col. 20, lines 1-25); and

unsecuring a cookie comprises: responsive to a request received through the

server interface for a cookie stored on a client computer (col. 18, lines 13-20), receiving

from the client computer the secured cookie corresponding to the requested cookie

through the at least one network interface (col. 20, lines 38-46); unsecuring the received

secured cookie by at least one of decrypting and hash verifying (col. 20, lines 16-21);

and providing the unsecured cookie through the server interface (col. 18, lines 61-65).

Therefore, one of ordinary skill in the art at the time the invention was made to

have incorporated Rollins within Wessman to include cookie in order to allow a web

server to identify repeat users or customers and to allow the web server to customize its

content based upon the user's preferences that are stored in the cookie (Rollins, col. 13,

lines 14-18).

7.   Claim 52 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Wessman (U.S. Patent 7,111,005 B1) hereinafter Wessman in view of Johnson (U.S.

Patent 6,898,577 B1) hereinafter Johnson.

8.

Regarding Claim 52, Wessman discloses a system for protecting sensitive data

stored in a web server environment, (Figures 1 and 2), comprising:

one or more clients coupled to at least network (Figures 1and 2, element 110);

a web server environment that stores data received from the web and does not

secure by encrypting, hashing, or keyed hashing the data received from the web before

it is stored (Figures 1and 2, element 118), and a transparent encryption appliance for

protecting sensitive data contained in the data stored in the web server environment

(Figures 1and 2, element 112), comprising:

at least one network interface for coupling to at least one network and

communicating with one or more clients via the at least one network (Figures 1 and 2,

interface between element 110 and 112);

a server interface for coupling to a web server environment, wherein the server

interface and the at least one network interface communicate using the same

communications protocol (Figures 1 and 2, interface between element 112 and 118);

and

a processor coupled to the at least one network interface and the server interface

for at least one of securing and unsecuring data (Figures 1 and 2, element 112),

wherein:

securing data comprises: identifying first sensitive data contained in a data

transaction received through the at least one network interface (col. 1, lines 15-17);

securing the sensitive data by at least one of encrypting, hashing, and keyed hashing

(Figure 6, element 602); replacing in the data transaction the identified sensitive data

with the secured sensitive data (Figure 6, element 610, col. 1, lines 15-17 and col. 6,

line 9); and providing the data transaction including the secured sensitive data to the

web server environment, wherein the secured sensitive data is stored in the web server environment (Figure 6, elements 606 and 612, col. 6, lines 10-12); and

unsecuring data comprises: responsive to a request (a request from client 110) received through the at least one network interface for sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data (Figure 7, element 702, col. 6, lines 17-18), receiving from the web server environment the secured sensitive data corresponding to the requested data (Figure 7, element 704, col. 6, lines 18-19); unsecuring the received secured data by at least one of decrypting and hash verifying (Figure 7, element 712, col. 6, lines 31-32); and providing the unsecured sensitive data through the at least one network interface (Figure 7, element 714, col. 6, lines 32-33).

Wessman does not disclose sensitive data as password and wherein, responsive to a request received through the at least one network interface of the appliance for an action requiring authorization, the web server environment obtains the secured password from the provided data transaction, compares the secured password to a previously stored secured password, and authenticates the action requiring authorization in the case the obtained secured password matches the previously stored secured password.

However, sensitive data as password (Abstract) and wherein, responsive to a request received through the at least one network interface of the appliance for an action requiring authorization, the web server environment obtains the secured password from the provided data transaction, compares the secured password to a

previously stored secured password (Figure 1B, step S15B, col. 7, lines 30-35), and

authenticates the action requiring authorization in the case the obtained secured

password matches the previously stored secured password (Figure 1B, steps S17B and

S18B, col. 7, lines 40-44).

Therefore, one of ordinary skill in the art at the time the invention was made to

have incorporated Johnson within Wessman to include above features in order to verify

the web customer's identity (Johnson, col. 7, lines 43-44).

Contact Information

9.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Baotran N. To whose telephone number is (571)272-

8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/B. N. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435